- TP 2 -
Accès distant par VPN

par Édouard Lumet

Introduction

Suite à des soucis techniques au niveau de Packet Tracer, je n'ai pas pu mener à bien le TP, en aucun point. En effet, après plusieurs vérifications des configurations Swicthes/Routeur, le DHCP ne fonctionne pas. De même pour la communication pourtant simple entre *PC fabrice* et *RouteurVPN* (le PC ne transmet pas les messages à sa gateway pour sortir du réseau alors que cette dernière lui est indiquée !!). Seules les explications théoriques seront ici abordées.

2. Configuration du réseau

Les liens inter-switches sont des trunk-VLANs. Ils permettent de faire transiter des données de différents VLANs sur un même VLAN, ce qui évite d'installer un lien physique par VLAN !

Le VLAN natif est le VLAN par défaut pour les trames non tagguées. Il faut absolument qu'il soit à part, c'est-à-dire non utilisé pour d'autres communications, surtout par l'accès au switch à distance (configuré par défaut sur le VLAN1).

3. Configuration de la communication inter-VLANs

Le lien SwitchCity1-RouteurVPN doit être configuré en mode trunk autorisant les VLANs 10, 20 et 30 pour permettre à tous les PCs d'emprunter ce lien.

L'encapsulation dot1Q (802.1Q) est un type de trame de couche 2 ajoutant des informations concernant le VLAN à une trame Ethernet classique (notamment le numéro de VLAN (tag VLAN) de la trame).

Un serveur DHCP permet à un hôte (équipement terminal de type PC) d'obtenir une adresse IPv4 de façon « automatisée ». L'utilisateur ou l'administrateur n'a pas besoin de configurer le PC en détail. Ce dernier configure seulement le serveur pour attribuer des lots d'adresses aux machines correspondantes.

La communication intra-VLAN est le dialogue entre deux machines appartenant au même VLAN alors que la communication inter-VLAN est le dialogue entre deux machines appartenant à deux VLANs différents.

4. Configuration de la connexion à distance

Sur le routeur VPN, on ajoute une route par défaut comme ceci :

ip route 0.0.0.0 0.0.0.0 fa0/1

Cela indique que les messages provenant de tous les réseaux non présents dans la table de routage seront dirigés en sortie via fa0/1, soit vers l'extérieur (routeur ISP).

5. Configuration de la connexion VPN

Les différentes commandes ont pour rôle de créer un pool d'adresses (et donc d'hôtes) étant accessible de l'extérieur via VPN, de créer une paire de clés et un utilisateur afin de chiffrer la connexion et de l'authentifier. Ici l'utilisateur est *user* avec le mot de passe *123*. Le tout est chiffré à l'aide d'un algorithme fort AES-256. On lie enfin le tout à l'interface fa0/1 qui est vers le monde extérieur, une des extrémités du tunnel VPN (l'autre sera le client à l'extérieur, comme *PC Fabrice* par ex).

Conclusion

Grâce à ce TP, nous avons appris à créer une connexion sécurisée (sur routeur Cisco) à distance entre un employé travaillant chez lui par exemple et l'entreprise qui l'emploi. En effet, cette connexion doit être particulièrement protégée car tout le trafic est routé à travers l'Internet, trafic provenant du réseau privé de l'entreprise.